

System health concepts

Published: 2019-02-10

You can assess the health and performance of an ExtraHop Discover appliance through system health tools. Monitoring system health data enables you to ensure that your Discover appliance is running as expected, to discover and troubleshoot issues, and to assess areas that need improvement. In addition, the ExtraHop Admin UI provides status information and diagnostic tools for all ExtraHop appliances.

Navigate the System Health page



The System Health page provides a large collection of charts with data such as packet throughput, heap allocation, and number of monitored devices. For example, you can monitor the number of packets processed by the ExtraHop system to ensure that packets are continuously captured. If you are sending data to a remote, third-party system through an open data stream (ODS), you can troubleshoot transmission errors to determine whether more memory should be dedicated to open data streams or whether an open data stream trigger requires modification.

Charts on the System Health page are divided into the following sections:

Capture

Displays charts that pertain to the health and performance of the wire data collected by the ExtraHop system.

Remote

Displays charts that pertain to the health and performance of open data stream (ODS) transmissions to a third-party syslog, database, or server.

Datastore

Displays charts that pertain to the health and performance of the ExtraHop datastore.

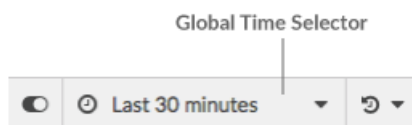
Trend

Displays charts that monitor performance and usage trends.

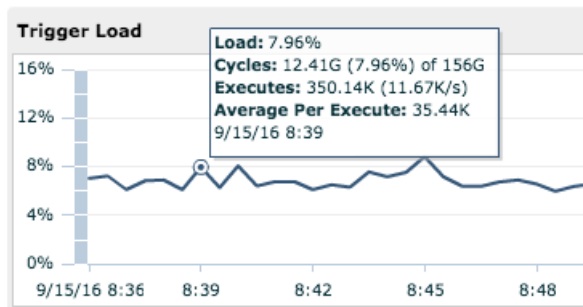
SSL certificates

Displays status information for all SSL certificates on the ExtraHop appliance.

Each chart enables you to view how the data changes over specified time intervals. The time interval selected in the Global Time Selector is applied to all charts on the page.




The sparklines on each chart contain data points that display additional details about a single point in time. Hover your mouse over a data point to display the additional details.



View Status and Diagnostics tools in the Admin UI

The Status and Diagnostics section of the ExtraHop Admin UI displays data about the ExtraHop appliance you are logged into and the wire data feed, and provides troubleshooting tools such as audit logs, exception files, and support packs. For example, you might want to monitor CPU statistics to determine whether CPU usage rates are within normal ranges. Or, you might want to consult audit logs to track down an issue.

The Admin UI is displayed by default when you log into an Explore or Trace appliance. To access the Admin UI from a Discover or Command appliance, click the System Settings icon , and then click Administration.

The Status and Diagnostics section includes the following pages:

Health statistics

Provides metrics to view the operating efficiency of the ExtraHop appliance.

Audit log

Enables you to view event logging data and to change syslog settings

Exception files

Enable or disable the creation ExtraHop appliance exception files.

Support packs

Upload and run ExtraHop appliance support packages.

Capture charts

The Capture section of the System Health page contains charts that pertain to the health and performance of the wire data collected by the ExtraHop system.

The Capture section provides the following charts:

- [Drops](#)
- [External timestamps](#)
- [Capture heap allocation](#)
- [Incoming packets breakdown](#)
- [Incoming throughput breakdown](#)
- [Packet capture disk throughput](#)
- [RPCAP packets](#)
- [RPCAP throughput](#)
- [TCP desyncs](#)
- [Trigger drops](#)
- [Trigger exceptions by trigger](#)
- [Trigger executes](#)
- [Trigger executes by trigger](#)

- [Trigger heap allocation](#)
- [Trigger load](#)
- [Trigger load by thread](#)
- [Trigger load by trigger](#)

Drops

Displays the percentage of packets dropped at the network card interface, SPAN, or network tap on an ExtraHop Discover appliance.

How this information can help you

Packet drops often result when appliance thresholds are exceeded. Refer to the [Datashheets](#) page to discover what the limits are for your ExtraHop Discover appliance. If the percentage of packet drops exceed 2%, contact [ExtraHop Support](#).

External timestamps

Displays the percentage of packets with an external timestamp read by the ExtraHop Discover appliance, based on the total number of packets processed.

How this information can help you

For internal purposes. The data in this chart might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Capture heap allocation

Displays the amount of memory, expressed in bytes, that the ExtraHop Discover appliance dedicates to network packet capture.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Incoming packets breakdown

Displays the rate of incoming packets, expressed in packets per second, on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of packets captured in the selected time interval.

Current

The number of packets captured during the most recent second.

Max

The maximum number of packets captured in the selected time interval.

The total, current, and maximum metrics are divided into the following categories:

Analyzed

The packets analyzed by the ExtraHop Discover appliance.

Filtered

The packets not included in network L2 metrics.

L2 duplicates

The identical Ethernet frames counted as duplicate L2 packets.

L3 duplicates

The identical TCP or UDP IPv4 packets counted as duplicate L3 packets.

How this information can help you

Exceeding product thresholds might result in data loss. For example, a high packet rate might result in packets dropped at the span source or at a span aggregator. Similarly, large amounts of L2 or L3 duplicates can also indicate an issue at the span source or span aggregator and might result in skewed or incorrect metrics.

The acceptable rate of packet per second depends on your product. Refer to the [Datasheets](#) page to discover what the limits are for your ExtraHop Discover appliance and determine if the rate of packets per second is too high.

Incoming throughput breakdown

Displays the throughput of incoming packets, expressed in bytes per second, on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of bytes transferred in the selected time interval.

Current

The number of bytes transferred during the most recent second.

Max

The maximum number of bytes transferred in the selected time interval.

The total, current, and maximum metrics are divided into the following categories:

Analyzed

The throughput analyzed by the ExtraHop Discover appliance.

Filtered

The throughput not included in network L2 metrics.

L2 duplicates

The identical Ethernet frames counted as duplicate L2 throughput.

L3 duplicates

The identical TCP or UDP IPv4 packets counted as duplicate L3 throughput.

How this information can help you

Exceeding product thresholds might result in data loss. For example, a high throughput rate might result in packets dropped at the span source or at a span aggregator. Similarly, large amount of L2 or L3 duplicates can also indicate an issue at the span source or span aggregator and might result in skewed or incorrect metrics.

The acceptable rate of bytes per second depends on your product. Refer to the [Datasheets](#) page to discover what the limits are for your ExtraHop Discover appliance and determine if the rate of bytes per second is too high.

Packet capture disk throughput

Displays the rate of bytes captured by the ExtraHop Discover appliance, expressed in bytes per second.

This chart also has the following metrics:

Total

The total number of bytes captured in the selected time interval.

Current

The number of bytes captured during the most recent second.

Max

The maximum number of bytes captured in a single second within the selected time interval.

How this information can help you

Monitor this chart for high amounts of throughput to the capture disk, which can indicate a large number of triggers with packet capture enabled. You might need to reassess the number of triggers or optimize packet capture triggers.

RPCAP packets

Displays the rate of remote packet capture (RPCAP) for all RPCAP peers, expressed in packets per second, on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of RPCAP packets captured in the selected time interval.

Current

The number of RPCAP packets captured during the most recent second.

Max

The maximum number of RPCAP packets captured in the selected time interval.

The total, current, and maximum metrics are divided into the following categories:

Encapsulation

The total number of RPCAP-encapsulated packets received by the Discover appliance.

Tunnel Eligible

The total number of RPCAP packets eligible to be forwarded to the Discover appliance.

Tunnel Sent

The total number of RPCAP-tunneled packets forwarded to the Discover appliance.

Tunnel Received

The total number of RPCAP-tunneled packets received by the Discover appliance.

The chart title contains the number of RPCAP peers. You can click the chart to open a second chart that displays the RPCAP packet metrics on a per-peer basis.

The RPCAP chart is only displayed if remote packet capture is enabled on the Discover appliance.

How this information can help you

Consult this chart after the initial setup of RPCAP to ensure that data is captured from every remote device on which RPCAP is deployed.

RPCAP throughput

Displays the rate of RPCAP throughput metrics for all RPCAP peers, expressed in bytes per second, on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of RPCAP bytes transferred in the selected time interval.

Current

The number of RPCAP bytes transferred during the most recent second.

Max

The maximum number of RPCAP bytes transferred in the selected time interval.

The total, current, and maximum metrics are divided into the following categories:

Encapsulation

The total number of RPCAP-encapsulated bytes received by the Discover appliance.

Tunnel Received

The total number of RPCAP-tunneled bytes received by the Discover appliance.

The chart title contains the number of RPCAP peers. You can click the chart to open a second chart that displays the RPCAP throughput metrics on a per-peer basis.

The RPCAP chart is only displayed if remote packet capture is enabled on the Discover appliance.

How this information can help you

Monitor this chart to ensure efficient usage of RPCAP resources and ensure that the Discover appliance can accommodate increases in RPCAP throughput.

TCP desyncs

Displays the occurrence rate of system-wide desyncs, expressed in desyncs per second, on the ExtraHop Discover appliance. A desync indicates that a transaction did not follow typical TCP behavior.

This chart also has the following metrics:

Total

The total number of desyncs that occurred in the selected time interval.

Current

The number of desyncs that occurred during the most recent second.

Max

The maximum number of desyncs that occurred in the selected time interval.

How this information can help you

A desync is recorded if synchronization is lost when processing a TCP connection. Large numbers of desyncs, such as over 100, might indicate dropped packets on the monitoring interface, SPAN, or network tap.

If adjustments to your SPAN does not reduce a large number of desyncs, contact [ExtraHop Support](#).

Trigger drops

Displays the number of triggers dropped from the queue of triggers waiting to run on the ExtraHop Discover appliance.

How this information can help you

Any data displayed on this chart indicates that trigger drops are occurring and that trigger queues are backed up.

The Discover appliance queues trigger operations if a trigger thread is overloaded. If the queue grows too long, the system stops adding trigger operations to the queue and drops the triggers. Currently running triggers are unaffected.

The primary cause of long queues, and subsequent trigger drops, is a long-running trigger.

Trigger exceptions by trigger

Displays the number of unhandled exceptions, sorted by trigger, that occurred on the ExtraHop Discover appliance. You can click the chart to open a second chart. This is the same secondary chart displayed from the Trigger Load by Trigger chart.

How this information can help you

Trigger exceptions are the primary cause of trigger performance issues. If this graph indicates a trigger exception has occurred, the trigger should be corrected immediately.

Trigger executes

Displays the number of times triggers were run per second during the selected time interval. The chart provides an overall snapshot of all triggers currently running on the ExtraHop Discover appliance.

How this information can help you

Look for spikes or an upward trend in the chart and investigate any triggers that have resulted in the surge. For example, you might notice increased activity if a trigger has been modified or a new trigger has been enabled. View the [Trigger executes by trigger](#) chart to see which triggers are running most frequently.

Trigger executes by trigger

Displays the number of times each active trigger ran during the selected time interval on the ExtraHop Discover appliance.

How this information can help you

Look for triggers that run significantly more frequently than average, which might indicate several issues. For example, a trigger assigned to all applications or all devices might have a heavy performance cost. A trigger assigned to a device group that has been expanded collect metrics you do not want. To minimize performance impact, a trigger should be assigned only to the specific sources that you need to collect data from.

High activity might also indicate that a trigger is working harder than it needs to. For example, a trigger might run on multiple events where it would be more efficient to create separate triggers, or a trigger script might not adhere to recommended scripting guidelines as described in the [Triggers Best Practices Guide](#) [↗](#).

Trigger heap allocation

Displays the amount of memory, expressed in bytes, that the ExtraHop Discover appliance dedicates to processing capture triggers.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Trigger load

Displays the percentage of cycles on the ExtraHop Discover appliance that are consumed by triggers based on the total capture thread time.

You can mouse over a point on the graph to display the following metrics:

Load

The trigger cycle load at the selected point in time.

Cycles

The number of consumed cycles out of the total available cycles.

Executes

The number of trigger operations and the average number of trigger operations per second.

Average per execute

The average number of cycles consumed per trigger operation.

How this information can help you

Look for spikes or upward growth of the trigger load, especially after creating a new trigger or modifying an existing trigger. If you notice either condition, view the [Trigger load by trigger](#) chart to see which triggers are consuming the most resources.

Trigger load by thread

Displays the percentage of trigger cycle consumption per thread that occurred on the ExtraHop Discover appliance, based on the total capture time of the thread.

How this information can help you

The sparklines on this chart should display an even amount of consumption among multiple threads. Trigger drops might occur if the consumption of one thread is considerably higher than the others, even if the thread consumption is at a low percentage. For example, if consumption on one thread is 10% and 25% on another, then consumption is uneven and you should contact [ExtraHop Support](#).

Trigger load by trigger

Displays the number of cycles consumed by each trigger enabled on the ExtraHop Discover appliance. You can click the chart to open a second chart that displays the consumption metrics on a per-trigger basis.

How this information can help you

Determine if any trigger appears to be consuming more cycles than average. If so, click to open the second chart and review the number of times the trigger has run. If the trigger has not run often, the trigger might be consuming more cycles than necessary, which can cause trigger drops.

Remote charts

The Remote section of the System Health page contains charts that pertain to the health and performance of open data stream (ODS) transmissions to a third-party syslog, database, or server.

The Remote section provides the following charts:

- [Connections](#)
- [Remote heap allocation](#)
- [Message errors](#)
- [Message queue length](#)
- [Message throughput](#)
- [Messages dropped](#)
- [Messages sent](#)

Connections

Displays the number of attempts by the ExtraHop Discover appliance to connect to remote, third-party systems through open data streams (ODS).

You can mouse over a point on the graph to display data in the following categories:

Connection attempts

The number of attempts to connect to the remote system.

Connection errors

The number of errors that occurred during attempts to connect to the remote system.

You can click the chart to open a second chart, which is the same secondary chart displayed from the [Messages sent](#) chart.

How this information can help you

Monitor this chart for an at-a-glance view of connection metrics. Consult the secondary chart to determine which ODS is experiencing connection issues. You can also monitor connection metrics from the [Messages sent](#) or [Message throughput](#) charts.

Remote heap allocation

Displays the amount of memory, expressed in bytes, that the ExtraHop Discover appliance dedicates to open data streams (ODS).

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Message errors

Displays the errors detected during the transmission of data from the ExtraHop Discover appliance to remote, third-party systems through an open data stream (ODS).

You can mouse over a point on the graph to display data in the following categories:

Send errors

The number of errors that occurred during the transmission of data to the remote system.

Parse errors

The number of times a message could not be sent due to encoding issues in the trigger script.

Bad targets

The number of times a remote system could not be located. Bad targets often occur when the name of the remote system specified in the trigger script does not match the name configured in the Admin UI.

Queue full

The number of times the message queue was full. A full queue occurs when the remote system cannot handle the current message rate.

You can click the chart to open a second chart, which is the same secondary chart displayed from the [Messages sent](#) chart.

How this information can help you

If you have noticed errors on either the [Messages sent](#) or [Message throughput](#) charts, consult this chart to determine the type of errors associated with an ODS. For example, send errors might require you to update the ODS configuration, and you might need to correct trigger script issues if you see parse errors.

Message queue length

Displays the number of messages in the internal message queue that are waiting to be sent through an open data stream (ODS) from the ExtraHop Discover appliance.

How this information can help you

A long message queue might indicate that the Discover appliance is sending data faster than the remote system can process and could result in dropped messages. Refer to the [Messages dropped](#) chart to determine if message drops have occurred.

Message throughput

Displays the throughput of message data, expressed in bytes per second, sent to remote, third-party systems from the ExtraHop Discover appliance through an open data stream (ODS).

This chart also has the following metrics:

Total

The total number of message bytes transferred during the selected time interval.

Current

The number of message bytes transferred during the most recent second.

Max

The maximum number of message bytes transferred during the selected time interval.

You can click the Message Throughput chart to open a second chart that displays the total number of message bytes transferred and the total number of message bytes seen by remote systems. The chart also displays the following information for each ODS:

Sent

The number of message bytes sent to the remote system.

Seen

The number of message bytes seen by the remote system.

Send errors

The number of errors that occurred during the transmission of data to the remote system.

Connection attempts

The number of attempts to connect to the remote system.

Connection errors

The number of errors that occurred during attempts to connect to the remote system.

Queue full

The number of times the queue was full because the remote system could not handle the current message rate.

How this information can help you

Monitor this chart to ensure that bytes are being transferred as expected. If no bytes are sent, there might be an issue with the configuration of an ODS or an ODS trigger.

Check for high numbers in the send errors, connection errors, and queue full counts, which might indicate problems with your data streams. Refer to the secondary chart to view which ODS configurations have errors and refer to the [Message errors](#) chart to view the error types that were generated.

Messages dropped

Displays the number of messages dropped from an Open Data Stream (ODS) because the internal message queue was full.

How this information can help you

Dropped messages might indicate that the ExtraHop Discover appliance is sending data faster than the remote system can process. A long queue can cause messages to drop. Refer to the [Message queue length](#) chart to determine if the wait for messages to be sent is unusually long.

Messages sent

Displays the number of messages per second that were sent to remote, third-party systems from the ExtraHop Discover appliance through an open data stream (ODS).

This chart also has the following metrics:

Total

The total number of messages sent during the selected time interval.

Current

The number of messages sent during the most recent second.

Max

The maximum number of messages sent during the selected time interval.

You can click the Messages Sent chart to open a second chart that displays the total number of messages sent and the total number of messages seen by remote systems both for all open data streams and for an individual open data stream. The chart also displays the following information about each ODS:

Sent

The number of messages sent to the remote system.

Seen

The number of messages seen by the remote system.

Send errors

The number of errors that occurred during the transmission of data to the remote system.

Connection attempts

The number of attempts to connect to the remote system.

Connection errors

The number of errors that occurred during attempts to connect to the remote system.

Queue full

The number of times the queue was full because the remote system could not handle the current message rate.

How this information can help you

Monitor this chart to ensure that packets are sent as expected. If no packets are sent, there might be an issue with the configuration of an open data stream or an open data stream trigger.

Check for high numbers in the send errors, connection errors, and queue full counts, which might indicate problems with your data streams. Refer to the secondary chart to view which open data streams have errors and refer to the [Message errors](#) chart to view the error types that were generated.

Datastore charts

The Datastore section of the System Health page contains charts that pertain to the health and performance of the ExtraHop datastore.

The Datastore section provides the following charts:

- [Active devices](#)

- Total devices
- Block object combinations
- Datastore disk read throughput
- Datastore disk write throughput
- Datastore heap allocation
- Datastore metric size
- Working set size
- Store lookback
- Store read throughput
- Store write throughput
- Datastore trigger drops
- Datastore trigger exceptions by trigger
- Datastore trigger executes
- Datastore trigger heap allocation
- Datastore trigger load
- Datastore trigger load by trigger

Active devices

Displays the total number of active L2, gateway, pseudo, custom, and L3 devices monitored by the ExtraHop system in the selected time interval.

This chart also has the following metrics:

Current

The number of active devices during the most recent second.

Average

The average number of active devices in the selected time interval.

Max

The maximum number of active devices in the selected time interval.

How this information can help you

Monitor this chart after making SPAN configuration changes to ensure that there were no unintended consequences that could put the ExtraHop system in a bad state. For example, accidental inclusion of a network can strain the limits of the ExtraHop system capabilities by consuming more resources, requiring more packet handling, and exceeding device limits, which results in poor performance. Check that the ExtraHop system is monitoring the expected number of active devices.

Total devices

Displays the total number of L2, gateway, pseudo, custom, and L3 devices monitored by the ExtraHop system, whether active or inactive, in the selected time interval.

This chart also has the following metrics:

Current

The number of devices during the most recent second.

Average

The average number of devices in the selected time interval.

Max

The maximum number of devices in the selected time interval.

How this information can help you

Monitor this chart after making SPAN configuration changes to ensure that there were no unintended consequences that could put the ExtraHop system in a bad state. For example, accidental inclusion of a network can strain the limits of the ExtraHop system capabilities by consuming more resources, requiring more packet handling, and exceeding device limits, which results in poor performance. Check that the ExtraHop system contains the expected number of total devices.

Block object combinations

Displays the number of block object combinations on the ExtraHop Discover appliance that occurred in a given time frame. Block object combinations occur when multiple portions of memory that contain metrics are combined.

How this information can help you

A high number of block object combinations might result from triggers that are creating a large amount of custom metrics or committing metrics to a high number of applications.

Datastore disk read throughput

Displays the disk read throughput rate, expressed in reads per second, on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of disk reads in the selected time interval.

Current

The number of disk reads during the most recent second.

Max

The maximum number of disk reads in the selected time interval.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Datastore disk write throughput

Displays the disk write throughput rate, expressed in writes per second, on the ExtraHop Discover appliance. The chart displays data for the selected time interval and for 1 hour, 5 minute, and 30 second intervals.

This chart also has the following metrics:

Total

The total number of disk writes in the selected time interval.

Current

The number of disk writes during the most recent second.

Max

The maximum number of disk writes in the selected time interval.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Datastore heap allocation

Displays the amount of memory that the ExtraHop Discover appliance dedicates to the datastore, expressed in bytes.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Datastore metric size

Displays the metric size distribution on the ExtraHop Discover appliance. You can click the Metric Size chart to open a second chart that displays the maximum size of each metric size.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Working set size

Displays the write cache working set size for metrics on the ExtraHop Discover appliance. The working set size indicates how many metrics can be written to the cache for the selected time interval and for 1 hour, 5 minute, and 30 second intervals.

This chart also has the following metrics:

Cycle

The primary time interval.

Current

The working set size during the most recent second.

Max

The maximum working set size in the selected time interval.

How this information can help you

The data on this chart might spike after trigger creation or trigger modification if the trigger script is not collecting metrics efficiently.

Store lookback

Displays the estimated datastore lookback metrics on the ExtraHop Discover appliance. Lookback metrics are available in 1 hour, 5 minute, and 30 second time intervals based on the write throughput rate, which is expressed in bytes per second.

How this information can help you

Refer to this chart to determine how far back you are able to look up historical data for given time intervals. For example, you might be able to look up 1 hour intervals of data as far back as 9 days.

Store read throughput

Displays the datastore read throughput rate, expressed in reads per second on the ExtraHop Discover appliance.

This chart also has the following metrics:

Total

The total number of datastore reads in the selected time interval.

Current

The number of datastore reads during the most recent second.

Max

The maximum number of datastore reads in the selected time interval.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Store write throughput

Displays the datastore write throughput rate, expressed in writes per second, on the ExtraHop Discover appliance. The chart displays data for the selected time interval and for 1 hour, 5 minute, and 30 second intervals.

This chart also has the following metrics:

Total

The total number of datastore writes in the selected time interval.

Current

The number of datastore writes during the most recent second.

Max

The maximum number of datastore writes in the selected time interval.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Datastore trigger drops

Displays the number of datastore-specific triggers dropped from the queue of triggers waiting to run on the ExtraHop Discover appliance.

How this information can help you

Any data displayed on this chart indicates that datastore trigger drops are occurring and that trigger queues are backed up.

The system queues trigger operations if a trigger thread is overloaded. If the datastore trigger queue grows too long, the system stops adding trigger operations to the queue and drops the triggers. Currently running triggers are unaffected.

The primary cause of long queues, and subsequent trigger drops, is a datastore long-running trigger.

Datastore trigger exceptions by trigger

Displays the number of unhandled exceptions caused by datastore-specific triggers on the ExtraHop Discover appliance. You can click the chart to open a second chart, which is the same secondary chart displayed from the Datastore Trigger Load by Trigger chart.

How this information can help you

Datastore trigger exceptions are the primary cause of trigger performance issues. If this graph indicates a trigger exception has occurred, the datastore trigger should be corrected immediately.

Datastore trigger executes

Displays the number of times datastore-specific triggers on the ExtraHop Discover appliance were run per second during the selected time interval.

How this information can help you

A single datastore trigger that runs often might indicate that the trigger has been assigned to all sources, such as applications or devices. To minimize performance impact, a trigger should be assigned only to the specific sources that you need to collect data from.

Refer to the secondary chart available from the [Datastore trigger load by trigger](#) chart to view which datastore triggers are running most frequently.

Datastore trigger heap allocation

Displays the amount of memory, expressed in bytes, that the ExtraHop Discover appliance dedicates to the datastore triggers.

How this information can help you

The data in this chart is for internal purposes and might be requested by [ExtraHop Support](#) to help you diagnose an issue.

Datastore trigger load

Displays the percentage of cycles consumed by datastore-specific triggers on the ExtraHop Discover appliance, based on the total capture thread time.

You can mouse over a point on the graph to display the following metrics:

Load

The trigger cycle load at the selected point in time.

Cycles

The number of consumed cycles out of the total available cycles.

Executes

The number of trigger operations and the average number of trigger operations per second.

Average per execute

The average number of cycles consumed per trigger operation.

How this information can help you

Look for spikes or upward growth of the datastore trigger load, especially after creating a new datastore trigger or modifying an existing datastore trigger. If you notice either, refer to the [Datastore trigger load by trigger](#) chart to see which datastore triggers are consuming the most resources.

Datastore trigger load by trigger

Displays the number of cycles consumed by each datastore-specific trigger that is enabled and running on the ExtraHop Discover appliance. You can click the chart to open a second chart that displays the consumption metrics on a per-trigger basis.

How this information can help you

Determine if any datastore trigger appears to be consuming more cycles than average. If so, click to open the second chart and look up the number of times the trigger has run. If the trigger has not run often, the trigger is consuming more cycles than necessary, which can cause datastore trigger drops.

Trend charts

The Trend section of the System Health page contains charts that monitor performance and usage trends.

The Trend section provides the following charts:

- [Performance overview](#)
- [Trend details](#)

Performance overview

Displays the percentage of trend resources consumed on the ExtraHop Discover appliance within the last hour, and the date and time of the last trend recorded.

How this information can help you

Monitor this data to determine whether the percentage of consumption by trends is efficient and allows for sufficient headroom.

Trend details

Displays the total processing time, expressed in milliseconds, for each trend on the ExtraHop Discover appliance during the last hour. The Trend Details chart also displays the trend type, such as alert or custom page.

How this information can help you

Monitor this chart for trends that have high processing times and assess the trend configuration. The trend type can help you locate the source of the trend data. You can also disable or enable a trend from this chart.

SSL certificates

The System Health page provides access to the SSL Certificates table, which displays a list of all certificates that perform decryption on the ExtraHop Discover appliance.

Click **Certificates** at the top of the System Health page. The SSL Certificates table displays the following status information for each certificate:

Decrypted

The number of sessions that were successfully decrypted.

Unsupported

The number of sessions that could not be decrypted with passive analysis, such as DHE key exchange.

Detached

The number of sessions that were not decrypted or only partially decrypted due to desyncs.

Passthrough

The number of sessions that were not decrypted due to hardware errors, such as those caused by exceeding the specifications of SSL acceleration hardware.

How this information can help you

Monitor this page to ensure that the correct SSL certificates are installed on the ExtraHop Discover appliance and are performing decryption as expected.

Status and diagnostics tools in the Admin UI

The Status and Diagnostics section provides metrics about the overall health of the ExtraHop Discover appliance and diagnostic tools that enable ExtraHop Support to troubleshoot system errors.

The Status and Diagnostics section includes the following tools:

- [Health statistics](#)
- [Audit log](#)
- [Exception files](#)
- [Support packs](#)

Health statistics

A Health page is available on any ExtraHop appliance that you log into, which provides a collection of metrics about the operation of that appliance.

If issues occur with the ExtraHop appliance, the following metrics on the Health page can help you to troubleshoot the problem and determine why the ExtraHop appliance is not performing as expected.

System status

Information about the system CPU usage and hard disk.

Bridge status

Information about the ExtraHop appliance bridge component.

Capture status

Information about the ExtraHop appliance network capture process.

Service status

Information about the status of ExtraHop appliance services such as alerts, trends, or exconfig.

Interface status

Information about the status of ExtraHop appliance system interfaces.

Partition status

Information about the non-volatile random-access memory (NVRAM) status and usage of ExtraHop appliance components.

For more information about the Health page, see the [ExtraHop Admin UI Guide](#).

How this information can help you

The information on this page helps you assess the performance of ExtraHop system services; however, it is most important to monitor the number of packets received in the Interface section. An extreme drop or stop in the number of received packets indicates a serious issue with the ExtraHop system and requires immediate resolution.

Audit log

An audit log is available on any ExtraHop appliance that you log into, which provides data about the operations and activity, broken down by component, for that appliance. The audit log lists all known events by timestamp, in reverse chronological order. In the Syslog Settings on the Audit Log page, you can configure where to send audit logs.

The ExtraHop appliance collects the following log data and reports the results on the Audit Log Activity page:

Time

The time when the event occurred.

User

The ExtraHop system user who initiated the logged event.

Operation

The ExtraHop system operation that generated the logged event.

Details

The outcome of the event, such as Success, Modified, Execute, or Failure. Each log entry also identifies the originating IP address, when available.

Component

The ExtraHop system component that is associated with the logged event.

For more information about the Audit Log page, see the [ExtraHop Admin UI Guide](#).

How this information can help you

After an issue with the ExtraHop appliance occurs, consult the audit log to view detailed diagnostic data to determine what might have caused the issue.

Exception files

If enabled, exception files are available on any ExtraHop appliance that you log into. When you enable the Exception File setting, a core file of the data stored in memory is written to the disk if the system unexpectedly stops or restarts. This file can help ExtraHop Support diagnose the issue.

For more information about exception files, see the [ExtraHop Admin UI Guide](#).

How this information can help you

Exception files are for internal purposes and might be requested by [ExtraHop Support](#) to help diagnose an issue.

Support packs

Support packs are available on any ExtraHop appliance that you log into. ExtraHop Support might provide a support pack that can apply a special setting, make a small adjustment to the ExtraHop appliance, or provide help with remote support or enhanced settings.

The Admin UI enables you to upload and run diagnostic support packages to discover issues on the ExtraHop system.

For more information about support packs, see the [ExtraHop Admin UI Guide](#).

How this information can help you

Support packs are for internal purposes and might be requested by [ExtraHop Support](#) to help diagnose an issue.